INFORMATION PROCESSOR

Publication number: WO0057290 (A1)
Publication date: 2000-09-28

Inventor(s): KITAHARA JUN [JP]; ASAHI TAKESHI [JP]
Applicant(s): HITACHI LTD [US]; KITAHARA JUN [JP]; ASAHI TAKESHI [JP]

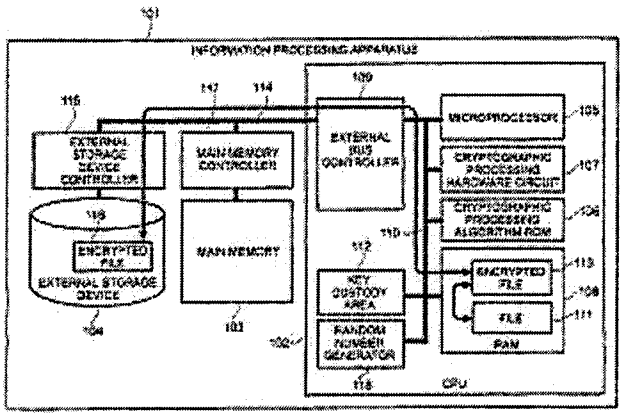
Classification:
- international: ***G06F21/00;*** *G06F12/14; G11B20/00;* **G06F21/00;** G06F12/14; G11B20/00; (IPC1-7): G06F15/00; G06F12/14; H04L9/10
- European: G06F21/00N1V3; G06F21/00N1C; G06F21/00N1C1
Application number: WO1999JP01402 19990319
Priority number(s): WO1999JP01402 19990319

Also published as:
US7082539 (B1)
JP3975677 (B2)
WO0057278 (A1)

Cited documents:
JP1004194 (A)
JP2297626 (A)
JP4149652 (A)
JP5314014 (A)
JP9044407 (A)

Abstract of **WO 0057290 (A1)**

A device structure is provided for carrying out safe encryption and decryption in information processors, communication devices and file management devices for security. Such devices are usually composed of a plurality of semiconductor devices, which may include secret data in its memory. An inventive structure comprises an integrated-circuit CPU that includes a microprocessor, a cryptographic algorithm ROM, cryptographic hardware, random access memory, key storage areas and an external bus control unit. Encryption and decryption are carried out only in the CPU, and the operation in the CPU cannot be inferred from signals outside the CPU.



Data supplied from the ***esp@cenet*** database — Worldwide

世界知的所有権機関
国際事務局

PCT

特許協力条約に基づいて公開された国際出願

(51) 国際特許分類6 G06F 15/00, 12/14, H04L 9/10	A1	(11) 国際公開番号	WO00/57290
		(43) 国際公開日	2000年9月28日(28.09.00)

(21) 国際出願番号 PCT/JP99/01402

(22) 国際出願日 1999年3月19日(19.03.99)

(71) 出願人（米国を除くすべての指定国について）
株式会社 日立製作所(HITACHI, LTD.)[JP/JP]
〒101-8010 東京都千代田区神田駿河台四丁目6番地
Tokyo, (JP)
(72) 発明者；および
(75) 発明者／出願人（米国についてのみ）
北原 潤(KITAHARA, Jun)[JP/JP]
朝日 猛(ASAHI, Takeshi)[JP/JP]
〒215-0013 神奈川県川崎市麻生区王禅寺1099番地
株式会社 日立製作所 システム開発研究所内 Kanagawa, (JP)
(74) 代理人
弁理士 作田康夫(SAKUTA, Yasuo)
〒100-8220 東京都千代田区丸の内一丁目5番1号
株式会社 日立製作所内 Tokyo, (JP)

(81) 指定国 CN, JP, KR, SG, US, 欧州特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE)

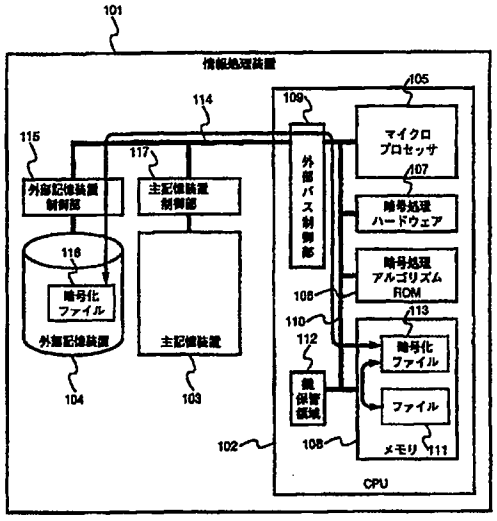
添付公開書類
国際調査報告書

(54)Title: INFORMATION PROCESSOR

(54)発明の名称 情報処理装置

(57) Abstract

A device structure is provided for carrying out safe encryption and decryption in information processors, communication devices and file management devices for security. Such devices are usually composed of a plurality of semiconductor devices, which may include secret data in its memory. An inventive structure comprises an integrated-circuit CPU that includes a microprocessor, a cryptographic algorithm ROM, cryptographic hardware, random access memory, key storage areas and an external bus control unit. Encryption and decryption are carried out only in the CPU, and the operation in the CPU cannot be inferred from signals outside the CPU.



101 ... INFORMATION PROCESSOR
103 ... MAIN STORAGE
104 ... EXTERNAL STORAGE
105 ... MICROPROCESSOR
106 ... CRYPTOGRAPHIC ALGORITHM ROM
107 ... CRYPTOGRAPHIC HARDWARE
108 ... MEMORY
109 ... EXTERNAL BUS CONTROLLER
111 ... FILE
112 ... KEY HOLDER
113 ... CODED FILE
115 ... EXTERNAL STORAGE CONTROLLER
116 ... CODED FILE
117 ... MAIN STORAGE CONTROLLER

(57)要約

本発明は、秘密保持のために、情報を暗号化／復号化する情報処理装置や通信装置やファイル管理装置において、安全に暗号化／復号化を行う装置構成を提供するものである。

これらの装置は、複数の半導体部品から構成されている。そのため、装置内のシステムバスや主記憶を構成する半導体記憶素子に秘密にすべきデータが存在してしまう問題点がある。

そこで、本発明は以下の構成をとる。各装置のCPUに、マイクロプロセッサと、暗号処理アルゴリズムROMと、暗号処理ハードウェアと、RAMと、鍵保管領域と、外部バス制御部を設けさらに同一半導体チップ上に集積する。このCPUを内でのみ暗号化／復号化処理を行い、さらにCPU内部動作をCPU外部信号から推測不可能にする。

明 細 書

情報処理装置

技術分野

本発明は、情報の保管、転送時の秘密性を保つために暗号を使用する情報処理装置に関する。その中でも特に、秘密性保持の高い情報処理を構築することに関する。

背景技術

暗号を使用する情報処理装置の従来技術としては、以下のものがある。

ハードディスクドライブのような外部記憶装置に、情報を暗号化して記憶するものとして、特開平１０－２７５１１５号公報がある。特開平１０－２７５１１５号公報では、外部記憶装置１２に一旦書き込まれた暗号化データＹａ，Ｙｂを情報端末装置１１へ転送する過程で、暗号化・復号鍵蓄積部３５に蓄積された復号鍵Ｋｂを用いながら当該暗号化データＹａ，Ｙｂに逐次的に復号処理を施すものである。

また、情報処理装置内に専用の暗号処理装置を設けたものとして、特開平１０－２１４２３３号公報がある。特開平１０－２１４２３３号公報では、携帯型ＰＣの中にデータを暗号化して暗号化ファイルのボディ部を生成する暗号化装置を備えている。

ここで、暗号化や復号化といった暗号処理は、一般に主記憶上のデータを対象に処理するため、主記憶上に秘密にすべきデータが存在する。情報を暗号化するためには、暗号アルゴリズムに従い情報を処理しなければならないが、暗号アルゴリズムと暗号に用いる鍵情報と暗号をかける秘密情

報全てを、安全に処理する必要が生じる。

しかし、これらの従来技術では以下の問題が存在する。

従来技術においては、秘密情報や暗号処理の途中経過が主記憶上に存在するため、幾つかの手法で情報を取り出す事が可能になる問題がある。この問題は、CPUや主記憶などが、複数の半導体で構成されている情報処理装置において、CPUを用いて暗号処理を行うと暗号アルゴリズムや暗号をかける秘密情報や暗号処理の途中経過が主記憶上に存在するためである。

また、情報処理装置内には、情報処理装置を構成する各半導体部品を接続する信号線（例えばバス）が存在するため、この信号線を観察し、情報を解析する事により、暗号化する前のデータや復号化したデータを簡単に取り出せるという問題がある。

発明の開示

上記の問題を解決するために、本発明では、以下の構成とした。

情報処理装置を構成する半導体内部で暗号化処理を施す。また、情報処理装置内の信号線上に暗号に関する情報を出力しない。情報処理装置の信号線上には、他者に観察されてもかまわない情報が出力される。この情報としては、暗号化された情報や暗号化する必要のない情報などである。なお、暗号に関する情報としては、暗号化されていない情報や暗号化された情報を復号するための情報を含む。

より具体的には、本発明の構成は、情報処理装置での処理を実行する処理装置（CPU）と同一半導体チップに、RAMと暗号処理アルゴリズムと暗号処理ハードウェアを集積したものである。なお、本明細書では便宜上CPUと読んでいるが、名称はこれに限られず、情報処理装置を構成する半導体チップであればよい。その中でも特に、情報処理装置の制御や演算処理を行う処理装置がよい。つまり、本発明は、情報処理装置を構成する１半導

体チップ内で暗号化処理が閉じているものである。さらに、本発明では、CPUが複数個あり、それぞれにおいて、暗号化処理が行う構成としてもよい。

また、この暗号処理が内蔵するRAM内で処理されてもよい。

また、CPUに内蔵されるRAMを主記憶として用い、アプリケーションプログラムの実行も内蔵するRAM内で処理されるものでもよい。

また、アプリケーションプログラム自体も暗号化され、外部記憶装置には、暗号化ファイルが存在する構成にしたものでもある。

また、外部バスへのデータ出力を制御する外部バス制御部を設けてもよい。この外部バス制御部では、内部RAMがアクセスされているときのデータを外部バスへ出力しないよう制御してもよい。さらに、このデータ外部バスに出力してもよい情報か否かを判断して、出力してもよい場合にデータを外部バスに出力するように制御してもよい。

また、通信データの暗号化／復号化をCPU内部で処理するものである。

さらに、これらのいずれかの構成に、情報に応じて暗号化するか否かを決定してもよい。情報が、暗号化しなくともよい情報であれば暗号化せずに情報処理装置の信号線上に出力する構成としてもよい。

さらに、本発明は、ディスクシステムコントローラ内のプロセッサ内部で暗号処理を可能にすることで、磁気ディスク上のファイル配置情報を暗号化したものも含まれる。

図面の簡単な説明

第１図は、本発明の情報処理装置の構成を示す図である。第２図は、本発明の情報処理装置におけるファイル生成を説明する図である。第３図は、本発明の１形態である主記憶を内蔵するCPUを有する情報処理装置の構成を示す図である。第４図は、本発明の１形態である外部記憶装置に格納しているアプリケーションプログラムをCPUで暗号化する情報処理装置の構成を

示すずである。第５図は、外部バス制御部の構成を示す図である。第６図は、外部バス制御部で外部バスへのデータを出力させない１実施例を説明する図である。第７図は、本発明をプロセッサバスおよびシステム情報処理装置に適用した場合の構成を示す図である。第８図は、本発明を通信に適用した場合の構成を示す図である。第９図は、外部記憶装置に本発明を適用した場合を説明する図である。第１０図は、第９図の構成で暗号化ファイル配置情報の書込みを説明する図である。第１１図は、ディスクコントローラの構成を示す図である。第１２図は、本発明の１形態である複数のCPUを有する情報処理装置を示す図である。第１３図は、第１２図の変形例を示す図である。第１４図は、第９図に示した構成の変形例である。第１５図は、第９図に示した構成の変形例である。第１６図は、第８図に示す情報処理装置がネットワークに接続されている全体システムを表わす図である。

発明を実施するための最良の形態

以下、図面を用いて本発明の実施例を説明する。

まず、本発明の第一の実施例を第１図および第２図を用いて説明する。第１図は、少なくとも、CPU(102)、主記憶装置(103)、外部記憶装置(104)を備える情報処理装置(101)の構成を模式的に表した図である。CPU(102)、主記憶装置制御部(117)、外部記憶装置制御部(115)は、理論上のシステムバス(114)で接続され、各々に主記憶装置(103)、外部記憶装置(104)が接続される。実際の信号線の接続は、第７図のようになるが、データの流れを理論的に考えると、模式的に第１図のように表す事が出来る。

CPU(102)は、マイクロプロセッサ(105)と、暗号処理アルゴリズムROM(106)と、暗号処理ハードウェア(107)と、RAM(108)と、鍵保管領域(112)と、外部バス制御部(109)からなる。さらに、同一半導体チップ上に

集積する。

CPU(102)内部では、マイクロプロセッサバス(110)に、暗号処理アルゴリズム ROM(106)と、暗号処理ハードウェア(107)と、RAM(108)と、外部バス制御部(109)が接続される。本実施例においては、CPU 内部でデータに対する暗号化処理が行われる。

ファイル(111)を暗号化するには、暗号処理アルゴリズム ROM(106)に従い、必要であれば暗号処理ハードウェア(107)を用いて暗号化する。この時の暗号化に用いる鍵データは、CPU(102)内で生成しても良いし、あらかじめ与えられるデータを用いても良い。但し、この鍵データは CPU(102)内の鍵保管領域(112)、保持されていなければならない。暗号化処理おいて、途中経過のデータが生成される場合は、その途中経過のデータも RAM(108)内に格納する。このようにして、ファイル(111)から暗号化ファイル(113)を生成する。

暗号化ファイル(113)は、システムバス(114)を通して外部記憶装置制御部(115)を経由して外部記憶装置(104)に格納する。

外部記憶装置(104)に格納されている暗号化ファイル(116)を復号化する場合は、逆の順序で処理を行う。

まず、外部記憶装置(104)から暗号化ファイル(116)を外部記憶装置制御部(115)を経由して RAM(108)に読み込む。次に、暗号処理アルゴリズム ROM(106)に従い、必要であれば暗号処理ハードウェア(107)を用いて復号化する。

大量のデータを高速に暗号化／復号化するためには、暗号鍵と復号鍵が共通である共通鍵暗号系を用いる。共通鍵暗号系では、暗号と復号は処理の順序が逆になっているだけで、最小単位の処理自体は暗号化も復号化も同じである。暗号処理アルゴリズム ROM(106)には、復号化処理の手順も格納しておく。また、暗号処理ハードウェア(107)は復号化でも使用する事が

可能である。

第２図は、第１図のファイル(111)を生成するまでの過程を示したものである。

アプリケーションプログラム(201)は、稼動時以外は外部記憶装置内に格納されている。このアプリケーションプログラムに起動がかかると主記憶に展開され動作可能な状態になる。動作可能になったアプリケーションプログラム(202)は、オペレーティングシステム等にの情報処理装置管理プログラムに対して、作業領域の割り当てを要求する。このとき、オペレーティングシステム等にの情報処理装置管理プログラムは、作業領域(203)としてRAM(108)内の空間を割り当てる。

この状態で、アプリケーションプログラム(202)は、マイクロプロセッサ(105)で処理され、生成された情報は作業領域(203)に格納される。この生成された情報の中から外部記憶装置に格納すべきデータをファイル(111)として生成する。

アプリケーションプログラム(202)自体は主記憶上に存在し、そのアプリケーションプログラムの作業領域(203)を RAM(108)上に取るためには、オペレーティングシステム等にの情報処理装置管理プログラムが管理するマイクロプロセッサが持つメモリ管理機能を用い、アプリケーションプログラムの作業領域を示す論理アドレスを RAM(108)内の物理アドレスに変換する事で可能になる。

鍵保持部(112)は、RAM(108)の領域内に設けられていても良いが、不揮発性でなければならない。EEPROM や FlashROM のような不揮発性の ROM で構成しても良いし、バッテリバックアップされた SRAM で構成しても良い。バッテリバックアップされた SRAM で構成した場合、暗号に使用した鍵を取り出そうと、情報処理装置に攻撃が加えられた場合にそれを検知し、バックアップ電源を切断する事で、鍵情報を消失させ秘密情報を守ることも可能

になる。

このように、情報の生成、暗号処理を同一半導体チップ内で行う事により、半導体チップの端子等の信号を観察するような解析方法でも、暗号のかからない秘密情報を入手する事は困難になる。

次に、本発明の第二の実施例を第３図を用いて説明する。

第３図は、CPU(101)内の RAM(108)を、情報処理装置(101)の主記憶として構成したものである。

この場合、外部記憶装置に格納されているアプリケーションプログラム(301)は、起動時に RAM(108)に展開され動作可能になる。動作可能になったアプリケーションプログラム(302)は、オペレーティングシステム等にの情報処理装置管理プログラムに対して、作業領域の割り当てを要求する。このとき、オペレーティングシステム等にの情報処理装置管理プログラムは、作業領域(303)として RAM(108)内の空間を割り当てる。この状態で、アプリケーションプログラム(302)は、マイクロプロセッサ(105)で処理され、生成された情報は作業領域(303)に格納される。この生成された情報の中から外部記憶装置に格納すべきデータをファイル(111)として生成する。

生成されたファイル(111)は、暗号処理アルゴリズム ROM(106)に従い、必要であれば暗号処理ハードウェア(107)を用いて暗号化される。暗号化されたファイル(113)は、外部記憶装置に暗号化ファイル(116)として格納される。

第３図では、CPU 外部の主記憶装置を図示していないが、秘密情報を生成するアプリケーションプログラムとそれ以外のアプリケーションプログラムを区別し、秘密情報を生成するアプリケーションプログラムの実行は、RAM(108)で行い、それ以外のアプリケーションプログラムは、従来通り CPU 外部の主記憶装置で処理する構成を取っても良い。

このように、RAM(108)を主記憶にする事により、CPU(102)外部にはアプ

リケーションプログラム(301)を RAM(108)に展開する時のデータ転送しか発生せず、アプリケーションプログラム自体の処理も安全に行える。

本発明の第三の実施例を第4図を用いて説明する。

本実施例では、暗号化されたアプリケーションプログラム(401)を外部記憶装置(104)に格納している。このアプリケーションプログラムは、情報処理装置の CPU 内で復号化される。このため、バス(114)上には、復号化されたアプリケーションプログラムは出力されず、復号化されたアプリケーションプログラムは CPU 内部で閉じている。このため、他者がこのアプリケーションプログラムを観察することを防止できる。

以下、第三の実施例の詳細を説明する。外部記憶装置内の暗号化アプリケーションプログラム(401)は、起動時にバス(114)を通して情報処理装置内の RAM(108)に転送される。転送された暗号化アプリケーションプログラム(402)は、RAM(108)に展開される。展開された暗号化アプリケーションプログラム(402)は、RAM(108)内で復号化され、アプリケーションプログラム(403)になる。この状態でアプリケーションプログラム(403)が動作し、RAM(108)内の作業領域(404)を用いながら情報を生成する。生成された情報は必要な部分が選択され、ファイル(111)としてまとめられる。ファイル(111)を暗号化し、暗号ファイル(113)を生成する。暗号ファイル(113)を暗号ファイル(116)として外部記憶装置(104)に格納する。

このように、アプリケーションプログラム自体も暗号化ファイルの一つとして外部記憶装置に格納する事により、さらに安全性を高める事も出来る。

なお、この暗号化アプリケーションプログラム(401)を生成するためには、アプリケーションプログラム自体をファイル(111)として、暗号化を行うものである。

次に、第5図および第6図を用いて、本発明の外部バス制御部の説明を

する。

第一から第三の各実施例に用いられる外部バス制御部(109)は、CPU内部と外部とのデータの入出力を制御するものである。例えば、マイクロプロセッサ(105)が行う、暗号処理のために暗号処理アルゴリズムROM(106)又は、暗号処理ハードウェア(107)又は、RAM(108)へのアクセスをCPU(102)外部に出ないように制御する。但し、マイクロプロセッサ(105)のアクセスがCPU外部に出力されても構わないものであれば、外部に出力されるよう制御してもよい。この場合、CPU外部に出力されても構わないデータとしては、暗号処理を行わず他の情報処理装置に転送するデータなどがある。

外部バス制御部(501)は、マイクロプロセッサ(502)の制御バス(503)、アドレスバス(504)、データバス(505)と、CPUの外部へ出る外部制御バス(506)、外部アドレスバス(507)、外部データバス(508)の間にあり、外部制御バス生成部(509)と、アドレス比較部(510)と、アドレス方向制御部(512)と、データ方向制御部(513)と、マスク信号生成部(511)と、信号マスク部(514)(519)から構成される。

制御バス(503)と外部制御バス(506)は、マイクロプロセッサからのバスサイクル開始信号、バス方向指示信号、バスサイクル終了信号、バス調停信号等が通される。これらの信号によりバスサイクルが制御される。

外部制御バス生成部(509)は、マイクロプロセッサからのバスサイクル開始信号、バス方向指示信号、バスサイクル終了信号、バス調停信号等を監視しする。外部制御バス生成部(509)は、マイクロプロセッサがバスアクセス権を所有しているか否かを判断し、その情報をアドレス方向制御部(512)に伝える。また、同じ情報をアドレス比較器(510)にも伝える。アドレス比較器(510)は、CPU(102)内部の暗号処理アルゴリズムROM(106)、暗号処理ハードウェア(107)、RAM(108)が割り当てられているアドレスを把握しており、アドレスバス(504)又は、外部アドレスバス(507)から入力されるアド

レスと比較する。

外部制御バス生成部(509)が制御バス(503)からマイクロプロセッサがバスアクセス権を所有していると判断すると、アドレス比較器(510)はマイクロプロセッサからのアドレスを監視し、RAM(108)のアドレスへのアクセスと検出すると、外部制御バス生成部(509)に伝えるえ、外部バス制御信号を駆動させない。また、マスク信号生成部(511)にも伝え、信号マスク部(514)(519)にマスク信号を出力し、外部アドレスバス(507)、外部データバス(508)を駆動しないように制御する。もしくは、強制的にアドレスの値やデータの値を固定してしまう。

外部制御バス生成部(509)が制御バス(503)からマイクロプロセッサがバスアクセス権を所有していないと判断すると、アドレス比較器(510)は外部アドレスバスを監視し、RAM(108)のアドレスへのアクセスと検出すると、外部制御バス生成部(509)に伝える。外部制御バス生成部(509)は、制御バス(503)へこのバスサイクルを伝達しない。もしくは、信号マスク部(514)(519)にマスク信号を出力し、アドレスバス(504)、データバス(505)を駆動しないように制御する。または、強制的にアドレスの値やデータの値を固定してしまう。

アドレスの値やデータの値を固定する方法として、第６図のように、信号マスク部(601)のゲート(602)と信号マスク部(603)のゲート(604)のように、ゲートの論理を変える事により実現できる。

このように、アドレス信号マスク回路で、RAM(108)領域以外の読み書きされても問題ない領域にアドレスを変換する事も可能である。

これにより、CPU(102)内部の処理をCPU(102)のバスであるシステムバス(114)を観察する事で推測する事が不可能になる。よって、CPU(102)内部で行う暗号処理の安全性が高まる。

次に、本発明の第四の実施例を第７図を用いて説明する。

第７図は、一般的な情報処理装置の構成を模式的に表した図である。

情報処理装置(701)は、複数の半導体部品から構成されいる。CPU(702)はプロセッサバス(704)で、キャッシュメモリと主記憶制御部(705)に接続される。主記憶制御部(705)は、システムバス制御部を含み、メモリバス(713)とシステムバス(707)が接続される。メモリバス(713)には、主記憶装置(706)が接続され、システムバス(707)には、外部記憶装置(708)、表示系制御部(710)、通信系制御部(711)、その他 I/O 制御部(712)が接続される。表示系制御部(710)は、専用バスで主記憶装置制御部＆システムバス制御部(705)に接続されていても良い。外部記憶装置制御部(708)には、外部記憶装置(709)が接続される。

主記憶装置(706)のアドレス領域と、システムバス(707)に接続される各部分のアドレス領域は異なっているため、アドレスでアクセスすべき領域を判断し、主記憶装置制御部＆システムバス制御部(705)が切り替えている。

このような、情報処理装置(701)では、情報処理装置を一つのシステムと捉えると、このシステム内の主となるプロセッサは、CPU(702)である。この CPU 内部で暗号化処理を閉じさせる。例えば、CPU(702)を図１のように、マイクロプロセッサ(105)と、暗号処理アルゴリズム ROM(106)と、暗号処理ハードウェア(107)と、RAM(108)と、鍵保管領域(112)と、外部バス制御部(109)で構成し、さらに、同一半導体チップ上に集積する。また、本発明は、第１２図および第１３図に示すとおり、複数のＣＰＵを有する情報処理装置であってもよい。

本発明の第五の実施例を第８図を用いて説明する。

第８図は、情報処理装置が他の情報処理装置と接続され、通信可能である構成を示す図である。ここでは、第１図の外部記憶装置の代わりに、通信系制御部を設けた構成をとる。なお、通信系制御部は、情報処理装置の外に接続されていてもよい。

情報処理装置(801)は、CPU(802)と、通信系制御部(803)とを備え、システムバス(814)で接続される。CPU(802)は、マイクロプロセッサ(805)、暗号処理アルゴリズムROM(806)、暗号処理ハードウェア(807)、RAM(808)、外部バス制御部(809)、鍵保管領域(812)から構成され、マイクロプロセッサバス(810)で接続される。

第８図では、情報処理装置は、CPUと通信系制御で構成されているが、他に主記憶や外部記憶装置等が備わっていても良い。通信系制御部(803)を経由した通信回線(804)の先に、外部記憶装置と同じ機能を持つ装置が接続されていても良いし、情報処理装置が接続されていても良い。

但し、通信回線(804)の先に接続される装置が、記憶装置か情報処理装置かで、暗号の掛け方が異なる。

通信回線の先に接続される装置が、外部記憶装置の場合、データを暗号化し、それを記憶装置に格納し、暗号化されたデータを記憶装置から読み出して復号化するものである。このため、暗号化に用いた鍵は、暗号化を行った情報処理装置のCPUだけが保持していれば良い。

通信回線の先に接続される装置が、情報処理装置の場合、通信回線を挟んで情報処理装置Aと情報処理装置Bが存在する。この場合、情報処理装置Aで情報を暗号化し、情報処理装置Bで情報を復号化する状況が生ずる。大量のデータを高速に暗号化／復号化するためには、共通鍵暗号系が適する。しかし、暗号化と復号化で同じ鍵を用いるため、情報処理装置AとBで、同じ鍵を所有していなければならない。この同じ鍵を、情報処理装置AとBであらかじめ設定しておいても良いし、暗号化したデータを送る前に、情報処理装置AとBで相互を行い、暗号化に用いた鍵を共有する方法を取っても良い。相互認証にも暗号処理が用いられるため、これらの処理は、CPU内部で処理される。

この情報処理装置ＡとＢがネットワークを介して接続されている様子を

第１６図に示す。

RAM(808)内で、暗号化したデータを通信単位に再編集し、通信プロトコルに従い、通信系制御部(803)に転送する事により、安全な通信が可能になる。RAM(808)内で暗号化したデータを通信系制御部(803)に転送し、通信系制御部(803)において、暗号化したデータを通信単位に再編集し、通信プロトコルに従い、通信路(804)にデータを送出しても良い。

本発明の第六の実施例を第９図、第１０図、第１１図、第１４図および第１５図を用いて説明する。

第９図は、磁気ディスク(901)等の外部記憶装置群を、ディスクシステムコントローラ(902)が制御する構成を取り、ディスクシステムコントローラ(902)は、上位の情報処理装置であるホストシステム(903)に接続されている。

磁気ディスク(901)内には、ファイルとして記憶されているデータと、そのファイルが磁気ディスク上の何処に格納されているかを示すファイル配置情報がある。PC 等の小型情報処理装置では、ファイルとファイル配置情報を管理するファイルシステムプログラムを、小型情報処理装置の CPU が処理する場合もあるが、高速動作や高信頼性を実現するディスクシステムコントローラでは、ディスクシステムコントローラ自体がファイルとファイル配置情報を管理する場合もある。

本実施例は後者に適用したものである。ホストシステム(903)では、ファイル(904)とファイル識別子(905)で管理する。ファイル(904)が暗号化されてるか否かは、ホストシステムに依存し、ディスクシステムコントローラでは関知しなくて良い。ディスクシステムコントローラ(902)では、磁気ディスク(901)上のファイル配置情報(906)を暗号化して管理する。

本実施例での、ホストシステムが暗号化した暗号化ファイル(907)を読み出すまでの動作を説明する。

まず、ホストシステムは、必要とする暗号化ファイルに対応するファイル識別子(905)をディスクシステムコントローラ(902)に送り、暗号化ファイルの読み出し要求を行う。読み出し要求を受けたディスクシステムコントローラ(902)は、磁気ディスク(901)から、暗号化されたファイル配置情報(906)を読み出し、ディスクシステムコントローラ(902)内で復号化し、ファイル配置情報(908)を取り出す。このファイル配置情報(908)内からファイル識別子(905)を検索し、実際のファイルの配置情報を得る。選られたファイル配置情報を用いて、要求された暗号化ファイル(907)を磁気ディスク(901)から読み出し、ホストシステム(903)へ転送する。

磁気ディスクにファイルを書き込む場合を第１０図で説明する。ファイル配置情報(908)を得るまでは、前記暗号化ファイルの読み出し動作と同じである。ファイル配置情報(908)から、磁気ディスク(901)の空き状態を確認し、磁気ディスク(901)空き領域に暗号化ファイル(904)を書き込む。書込み終了後、ファイル配置情報(908)を更新し、暗号化した後、磁気ディスク(901)に暗号化ファイル配置情報(1001)として書き込む。

第１１図で、ディスクシステムコントローラの構成を説明する。

本発明のディスクシステムコントローラ(1101)は、内部にディスクシステムのCPU(1102)と、磁気ディスクインタフェース(1113)と、ホストシステムインタフェース(1104)を持ち、CPU(1102)は、マイクロプロセッサ(1105)と、暗号処理アルゴリズムROM(1106)と、暗号処理ハードウェア(1107)と、RAM(1108)と、鍵保管領域(1111)と、外部バス制御部(1109)で構成される。

なお、第１４図および第１５図に示す通り、１台の情報処理装置に複数の磁気ディスク装置が接続される構成としてもよい。

このような、ディスクシステムコントローラを用いる事により、磁気ディスク内の情報を全て暗号化する事が可能になり、情報保管時の安全性

が高まる。

本発明の暗号処理ハードウェアは、暗号化と復号化において共通の鍵を用いる共通鍵暗号では、専用のハードウェアであり、ローテータ、加算器、論理演算器等で構成される。共通鍵暗号としては、あるデータ長を単位に、ビットのローテートと加算と論理演算を主演算とした暗号化手段である Multi 系の暗号、M6 暗号等を用いる事も出来る。

公開鍵暗号を用いる場合は、演算量の大きい剰余演算器を専用のハードウェアとして設ける。

産業上の利用可能性

本発明によれば、情報処理装置内のシステムバスやプロセッサバスにも秘密情報を出さずに、暗号処理が可能になる。

暗号処理とその処理に関する秘密情報、暗号アルゴリズム、途中経過、鍵情報等が、同一半導体内で処理されるため、秘密保持効果が高い情報処理装置を構築できる。

請 求 の 範 囲

1．情報に対して所定の処理を施す制御装置と、

前記制御装置と当該情報処理装置を構成する他の装置を接続するバスを有する情報処理装置において、

前記制御装置は、暗号化すべき情報の暗号化を当該制御装置を含む半導体チップ内で実行することを特徴とする情報処理装置。

2．請求項1に記載の情報処理装置において、

前記制御装置は、暗号化されていない情報を前記バスへの出力されないよう制御する外部バス制御装置を有することを特徴とする情報処理装置。

3．請求項2に記載の情報処理装置において、

前記外部バス制御装置は、暗号化しなくともよい情報は、前記バスへ出力することを特徴とする情報処理装置。

4．請求項1に記載の情報処理装置において、

前記制御装置で暗号化された情報を格納する記憶装置を有することを特徴とする情報処理装置。

5．請求項1に記載の情報処理装置において、

前記制御装置は、暗号化された情報を復号化する手段を有することを特徴とする手段を有することを特徴とする情報処理装置。

6．請求項5に記載の情報処理装置において、

ネットワークを介して他の情報処理装置と接続され、他の情報処理装置で暗号化されて送信された情報を前記制御装置で復号化することを特徴とする情報処理装置。

7．請求項1に記載の情報処理装置において、

前記処理装置を複数個有し、夫々の処理装置にて暗号化を行うことを特

徴とする情報処理装置。

8．請求項１に記載の情報処理装置において、

前記処理装置は、暗号化されたプログラムを受信し、復号化を施す手段を有することを特徴とする情報処理装置。

9．請求項１に記載の情報処理装置において、

前記処理装置は、前記所定の処理を実行するマイクロプロセッサと、

前記情報の暗号化処理のアルゴリズムが格納された暗号処理アルゴリズム格納装置と、

前記アルゴリズムに従って暗号化処理を実行する暗号化装置と、

前記マイクロプロセッサ、暗号処理アルゴリズム格納装置および前記暗号化装置それぞれを接続するマイクロプロセッサバスと

を有することを特徴とする情報処理装置。

10. 情報を処理する処理装置を有し、暗号化された暗号化情報を格納する磁気ディスクを制御するディスクシステムコントローラにおいて、

前記暗号化情報の読み出し要求を受け取った場合、前記磁気ディスクに格納された情報の配置を示す暗号化されている暗号化ファイル配置情報を、前記磁気ディスクから読み出し、読み出した暗号化ファイル配置情報を前記処理装置を含む半導体チップ内で復号化をし、復号化されたファイル配置情報に基づいて、前記暗号化情報を読み出すことを特徴とするディスクシステムコントローラ。

11. 請求項１０に記載ディスクシステムコントローラにおいて、

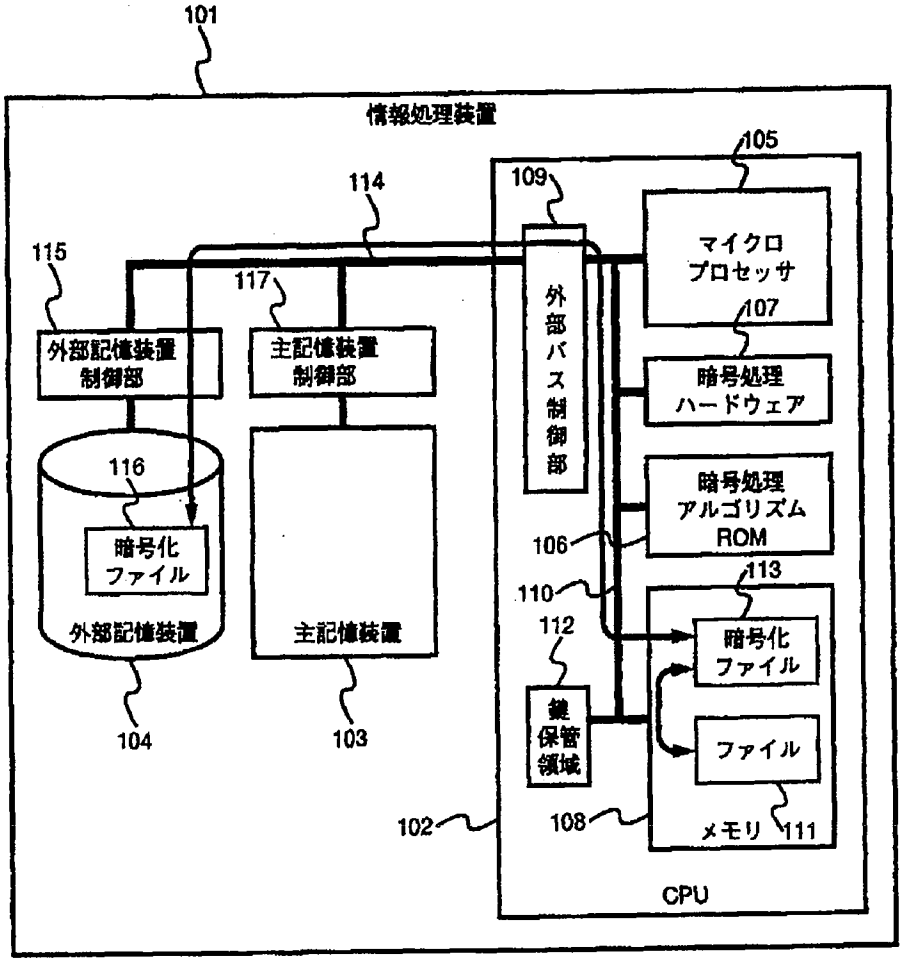
当該デ複数の磁気ディスクに接続されていることを特徴とするディスクシステムコントローラ。

12. 請求項１０に記載ディスクシステムコントローラにおいて、

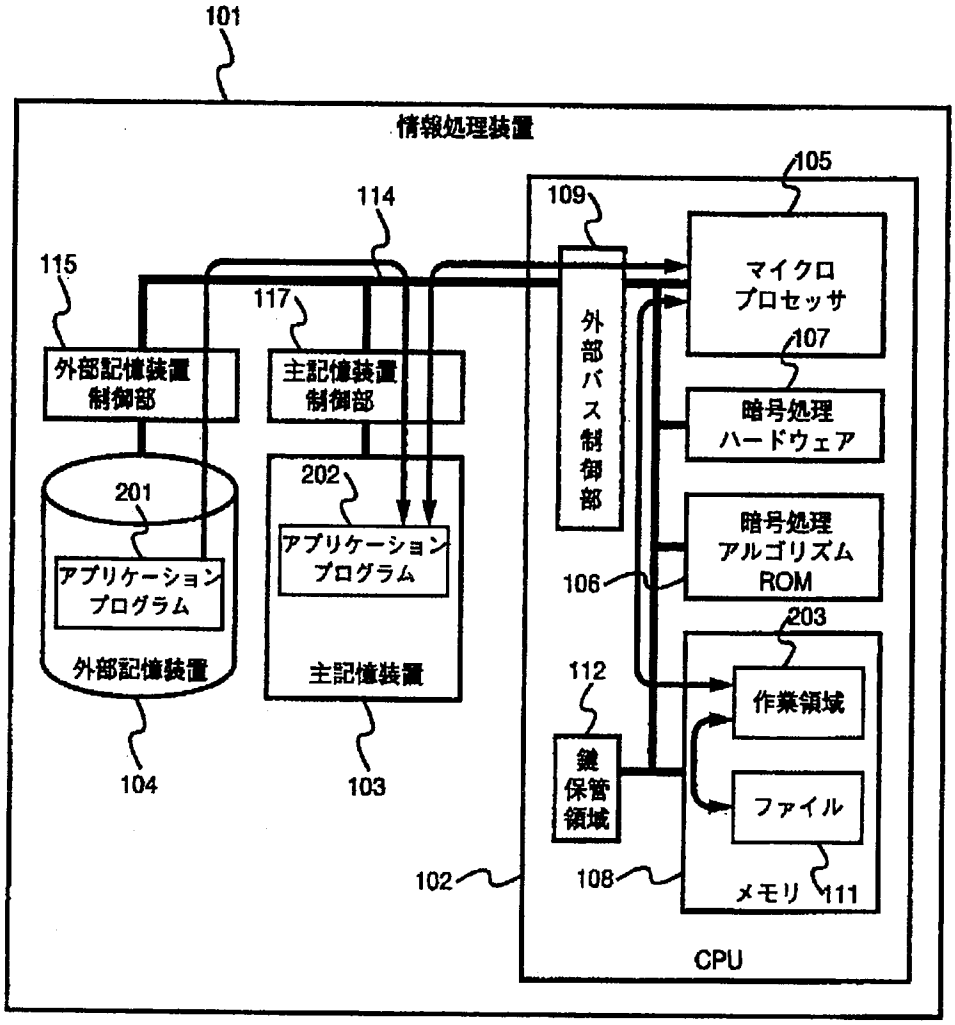
当該ディスクシステムコントローラは、情報処理装置に接続されており、前記情報処理装置からの要求により、前記暗号化情報を読み出すことを特

徴とするディスクコシステムントローラ。

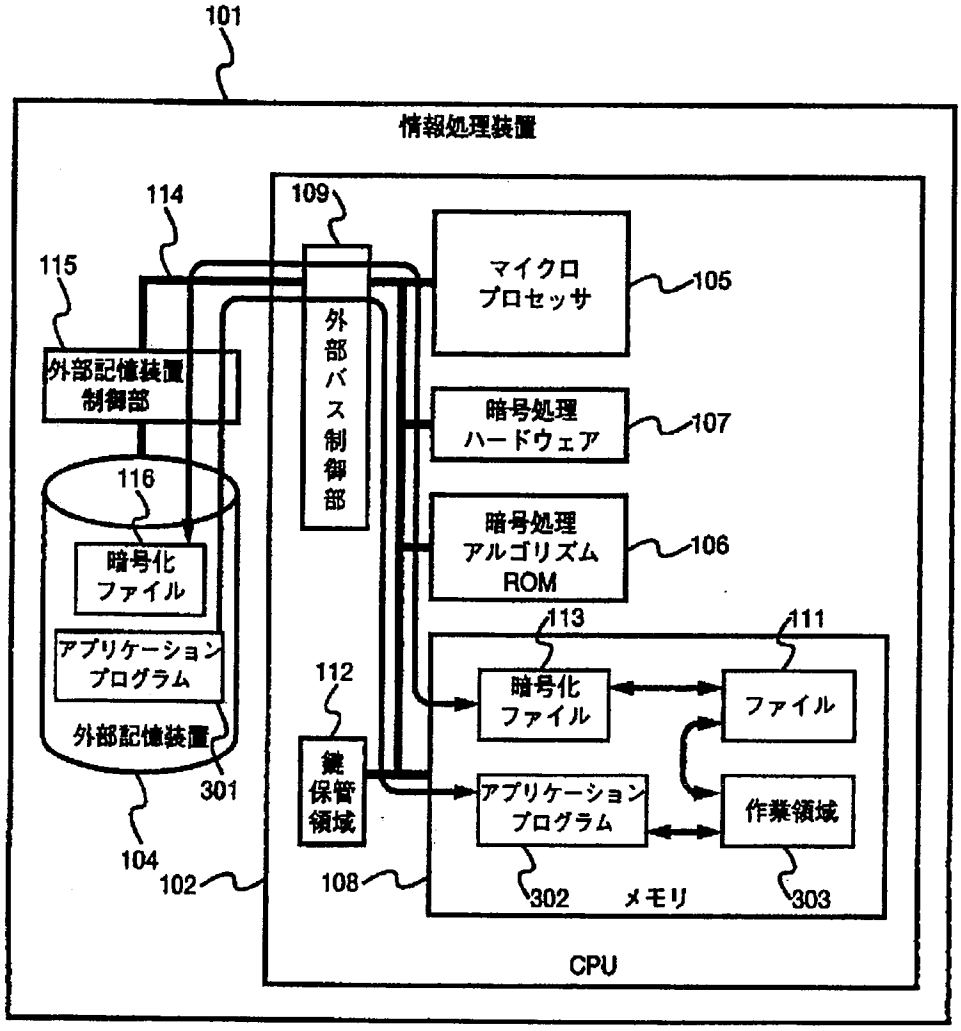
第1図


101
情報処理装置
105
109
114
マイクロ
プロセッサ
115
117
外部バス制御部
107
外部記憶装置
制御部
主記憶装置
制御部
暗号処理
ハードウェア
116
暗号処理
アルゴリズム
ROM
暗号化
ファイル
106
113
110
112
暗号化
ファイル
外部記憶装置
主記憶装置
鍵
保管
領域
ファイル
104
103
102
108
メモリ
111
CPU

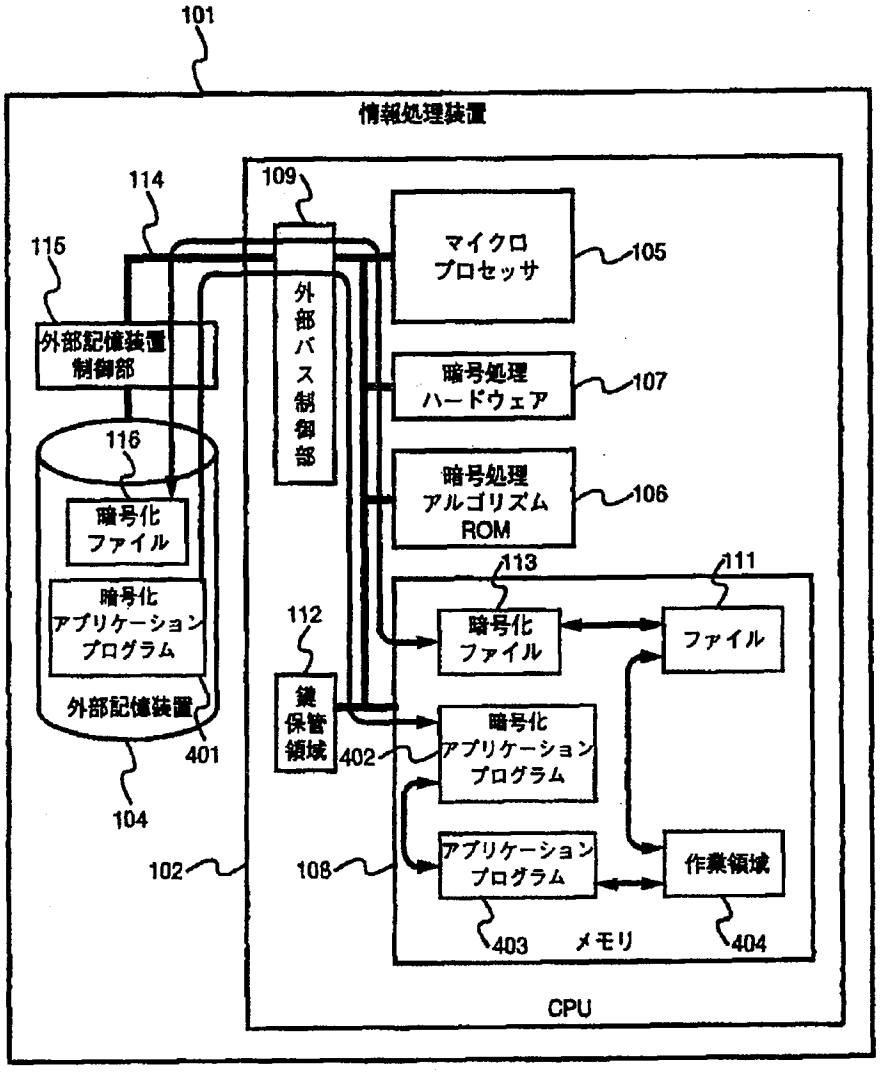
第２図


101
情報処理装置
105
109
114
115
117
外部記憶装置制御部
主記憶装置制御部
外部バス制御部
マイクロプロセッサ
107
暗号処理ハードウェア
暗号処理アルゴリズムROM
106
203
201
アプリケーションプログラム
外部記憶装置
202
アプリケーションプログラム
主記憶装置
112
鍵保管領域
作業領域
ファイル
メモリ
111
104
103
102
108
CPU

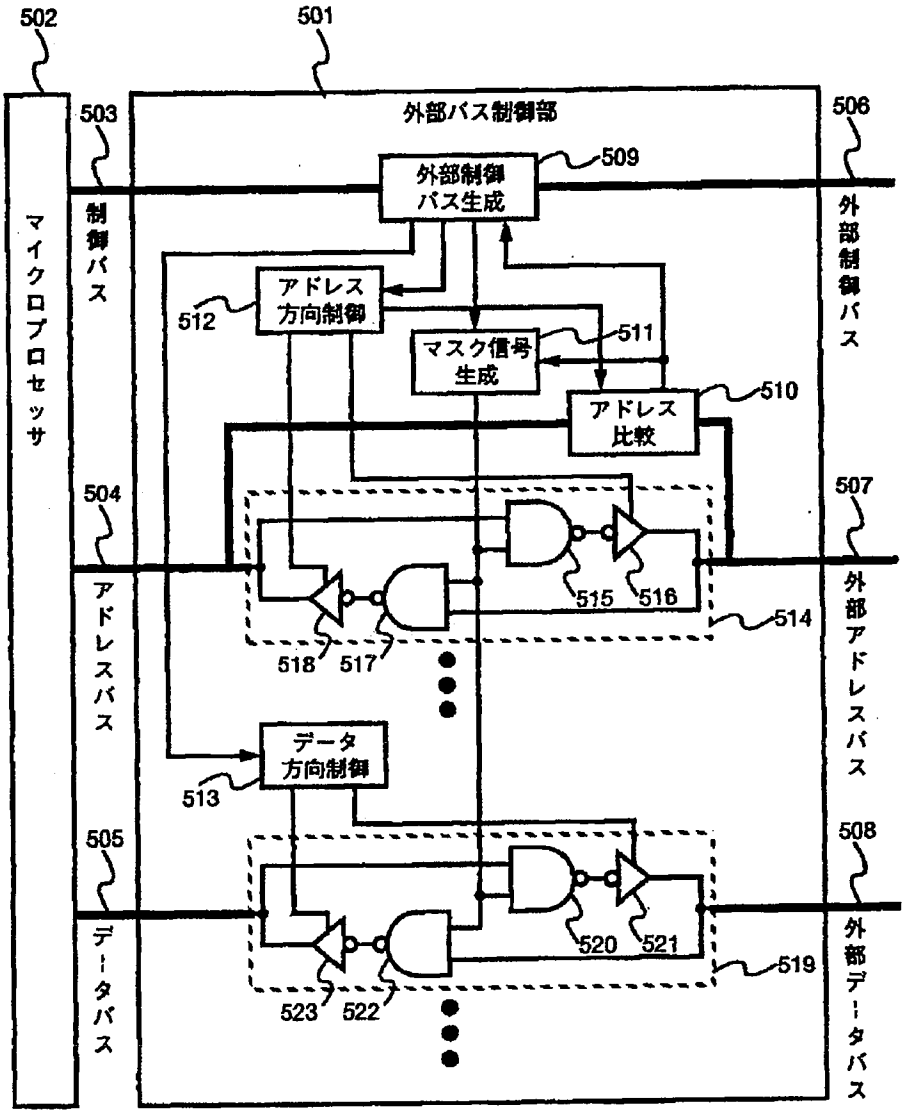
第３図


101
情報処理装置
114
109
115
マイクロ
プロセッサ
105
外部記憶装置
制御部
外部
バス
制御
部
暗号処理
ハードウェア
107
116
暗号処理
アルゴリズム
ROM
106
暗号化
ファイル
113
111
アプリケーション
プログラム
112
暗号化
ファイル
ファイル
外部記憶装置
鍵
保管
領域
アプリケーション
プログラム
作業領域
301
104
102
108
302
メモリ
303
CPU

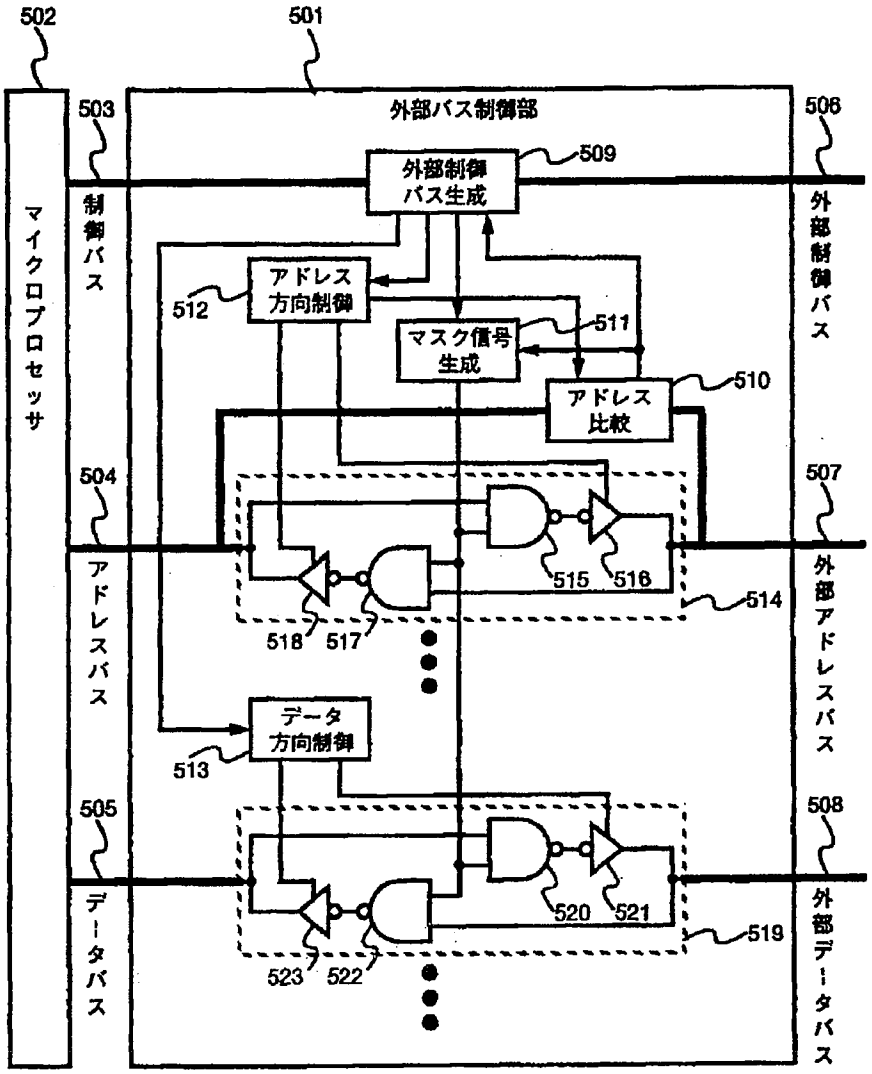
第４図


101
情報処理装置
114
109
115
マイクロ
プロセッサ
105
外部バス制御部
外部記憶装置
制御部
暗号処理
ハードウェア
107
116
暗号処理
アルゴリズム
ROM
106
暗号化
ファイル
113
111
暗号化
アプリケーション
プログラム
112
暗号化
ファイル
ファイル
鍵
保管
領域
外部記憶装置
暗号化
アプリケーション
プログラム
402
401
104
102
108
アプリケーション
プログラム
作業領域
403
メモリ
404
CPU

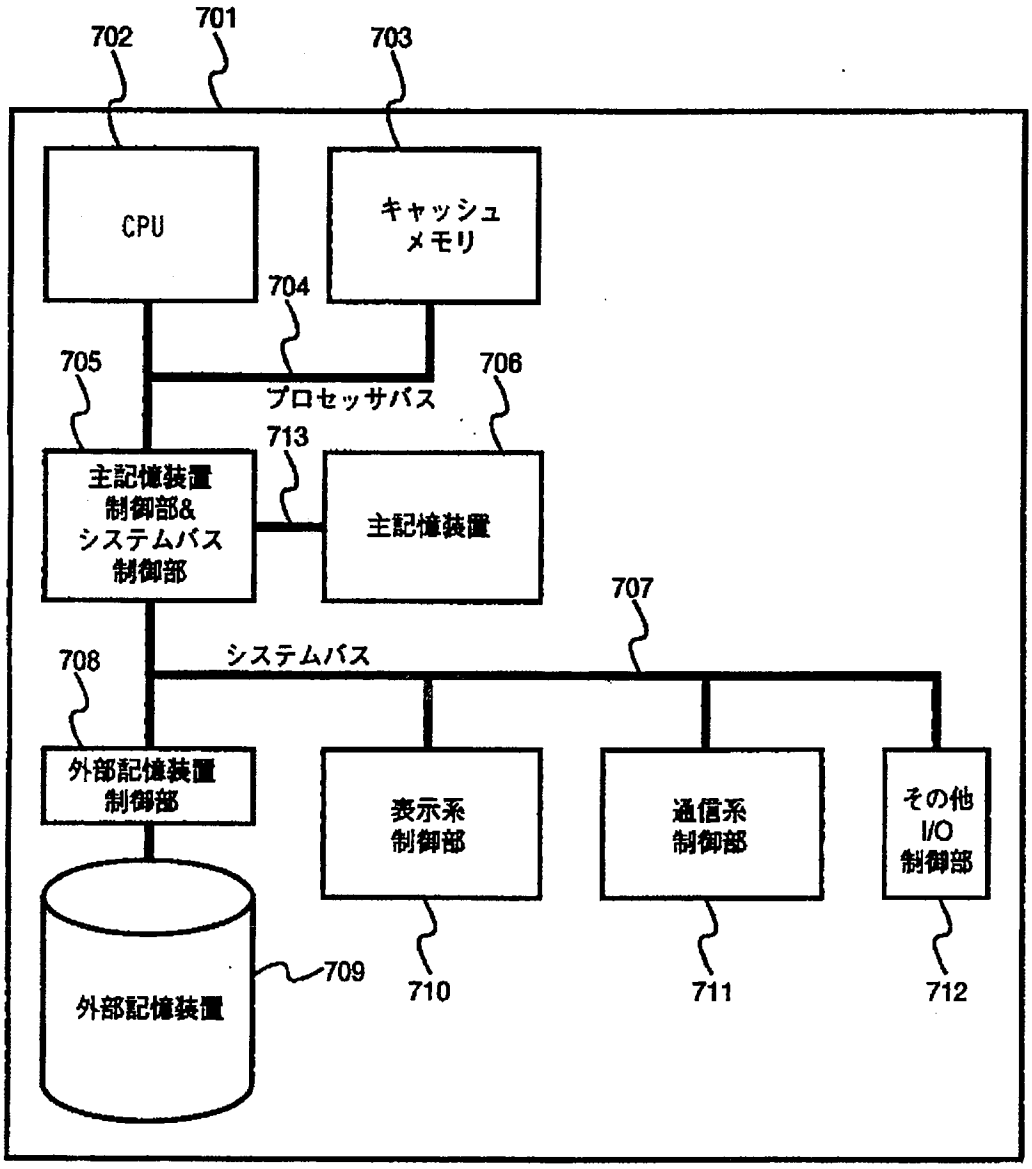
第５図


502
501
503
外部バス制御部
506
マイクロプロセッサ
制御バス
外部制御バス
509
外部制御バス生成
アドレス方向制御
512
マスク信号生成
511
510
アドレス比較
504
507
アドレスバス
外部アドレスバス
515
516
514
518
517
データ方向制御
513
505
508
データバス
外部データバス
520
521
519
523
522

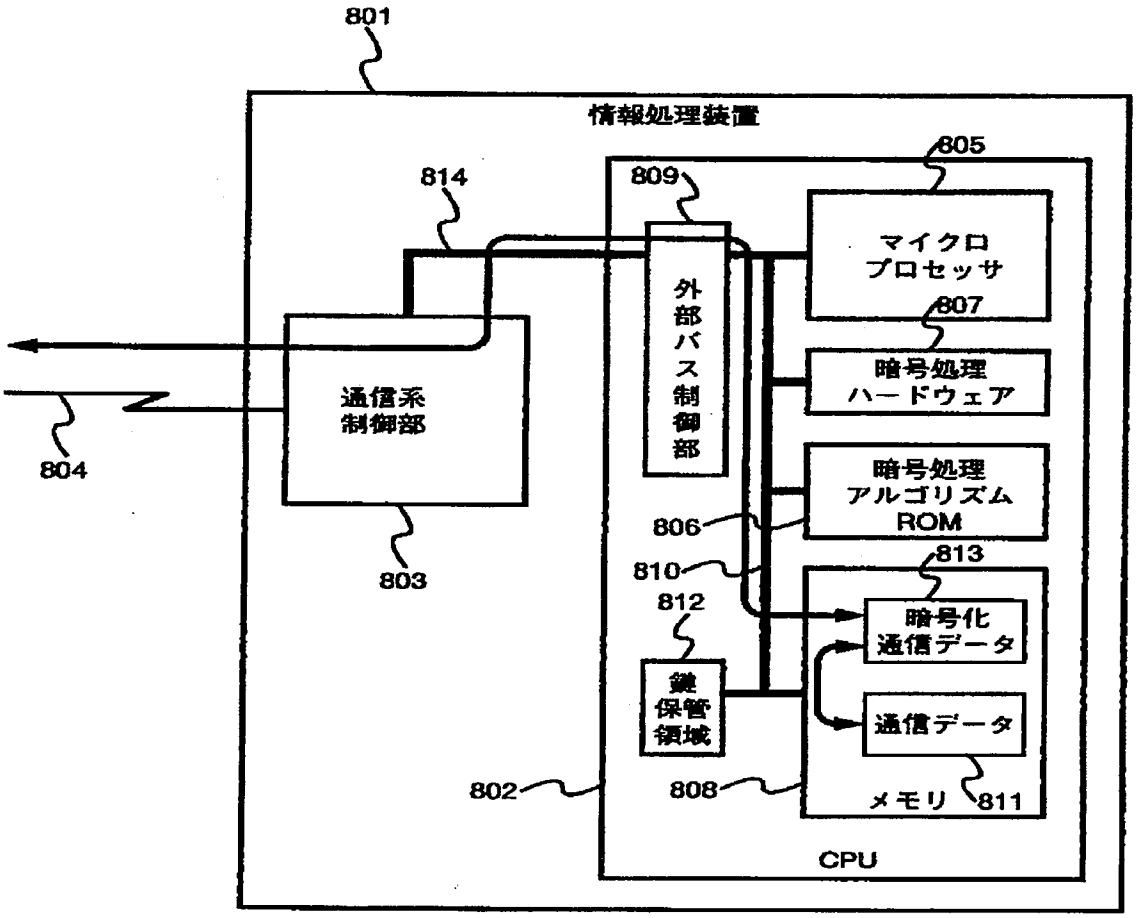
第6図


502
501
503
外部バス制御部
506
外部制御バス生成
509
マイクロプロセッサ
制御バス
外部制御バス
アドレス方向制御
512
マスク信号生成
511
アドレス比較
510
504
507
アドレスバス
外部アドレスバス
515
516
514
518
517
データ方向制御
513
505
508
データバス
外部データバス
520
521
519
523
522

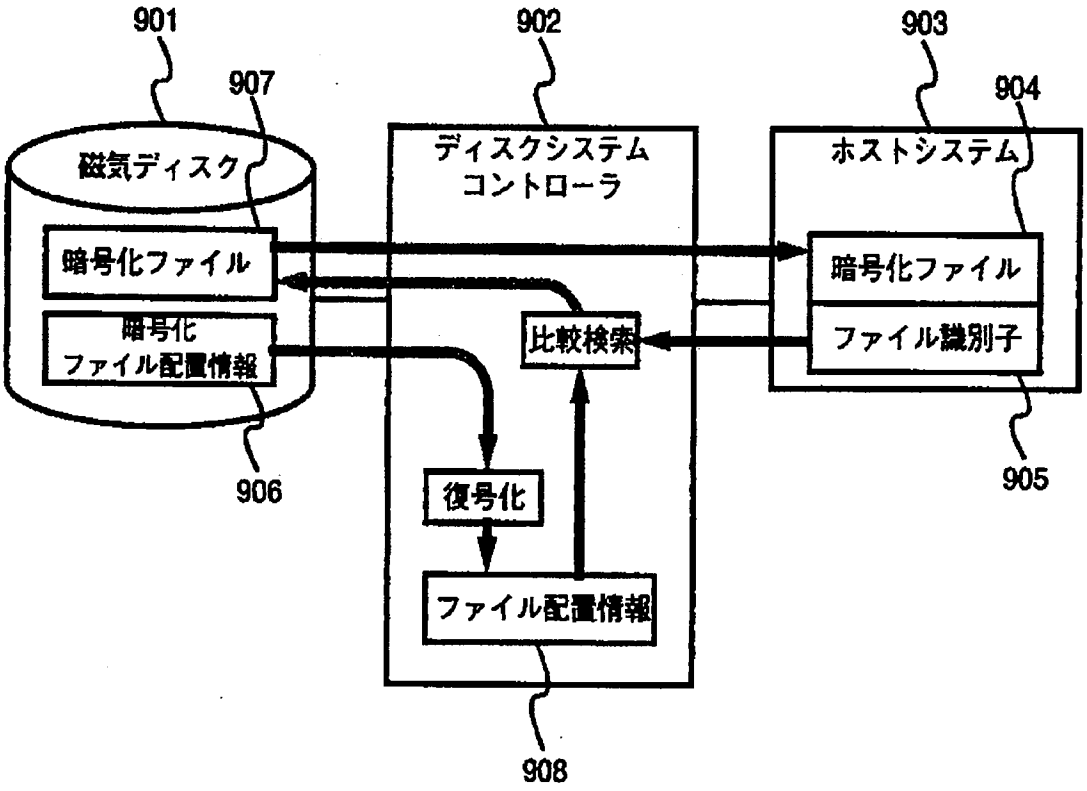
第７図


701
702
703
CPU
キャッシュ
メモリ
704
プロセッサバス
705
706
713
主記憶装置
制御部&
システムバス
制御部
主記憶装置
707
システムバス
708
外部記憶装置
制御部
表示系
制御部
通信系
制御部
その他
I/O
制御部
外部記憶装置
709
710
711
712

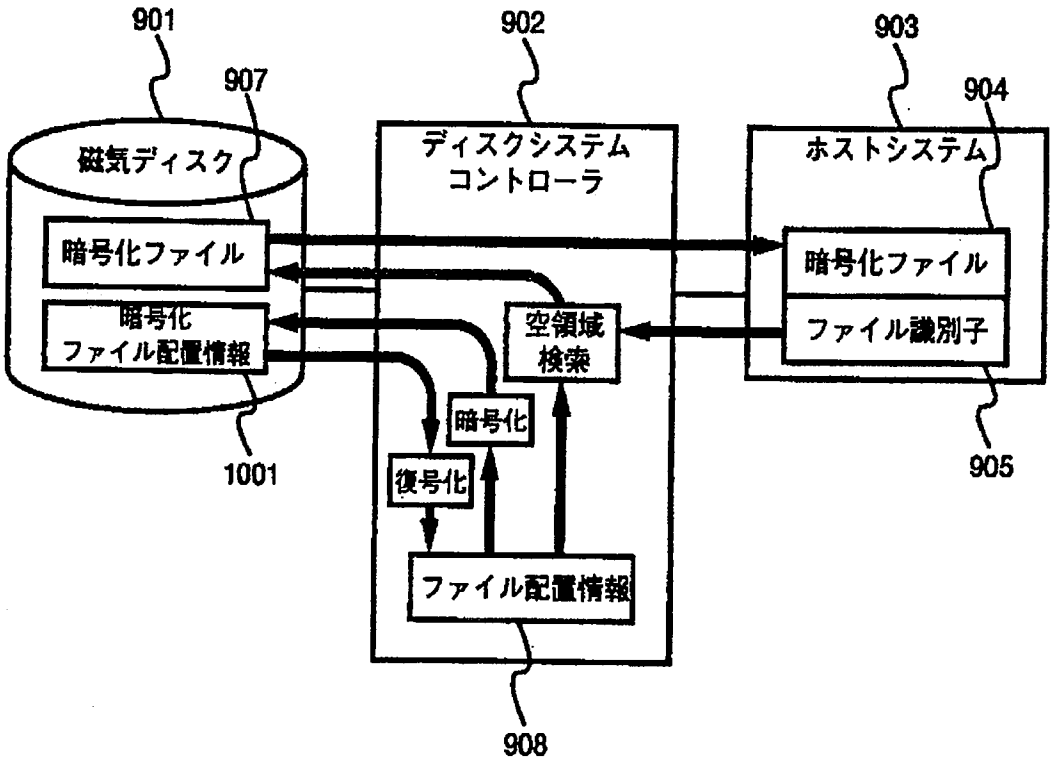
第８図


801
情報処理装置
805
809
814
マイクロ
プロセッサ
外
部
バ
ス
制
御
部
807
暗号処理
ハードウェア
通信系
制御部
804
暗号処理
アルゴリズム
ROM
803
806
813
810
812
暗号化
通信データ
鍵
保管
領域
通信データ
802
808
メモリ
811
CPU

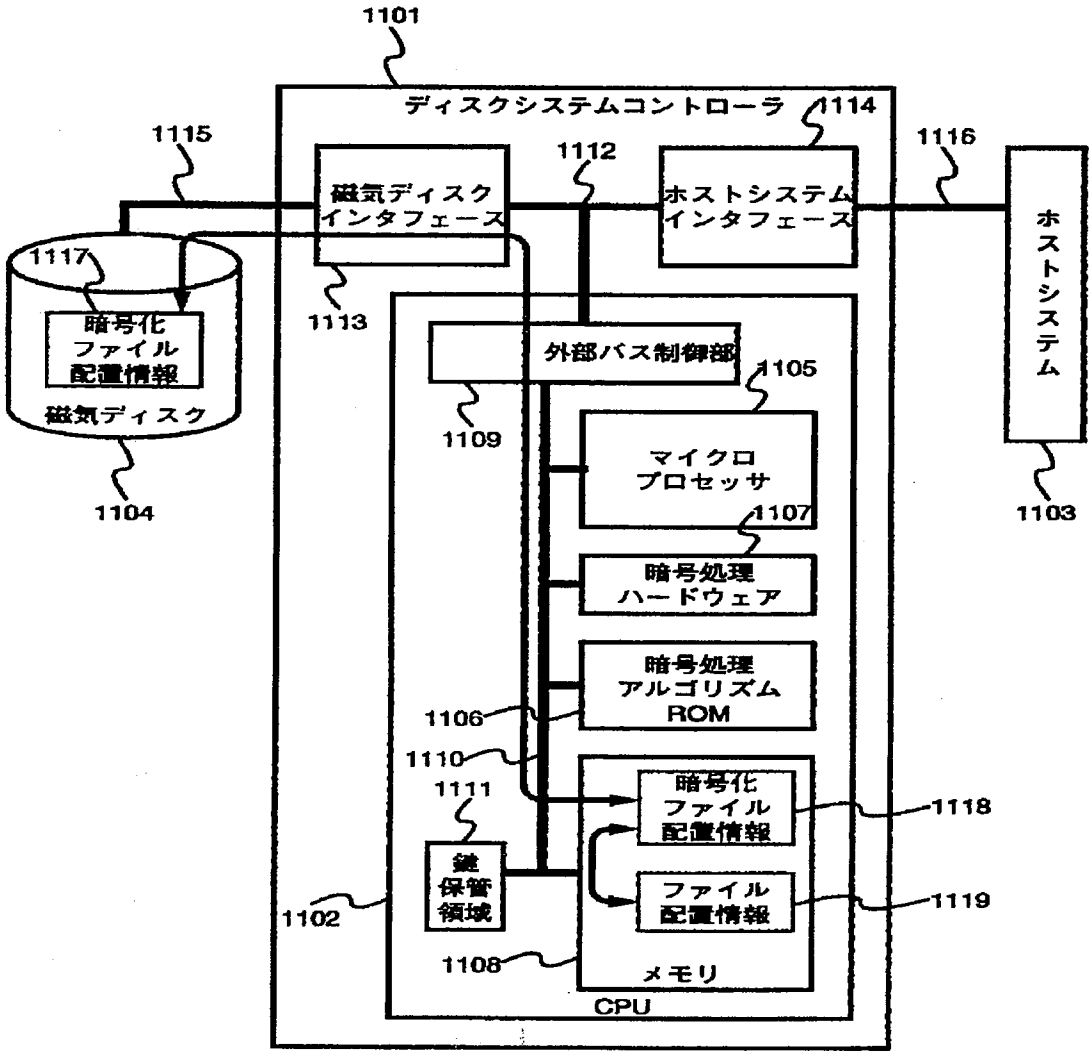
第９図


901
902
903
907
904
磁気ディスク
ディスクシステム
コントローラ
ホストシステム
暗号化ファイル
暗号化
ファイル配置情報
比較検索
暗号化ファイル
ファイル識別子
906
905
復号化
ファイル配置情報
908

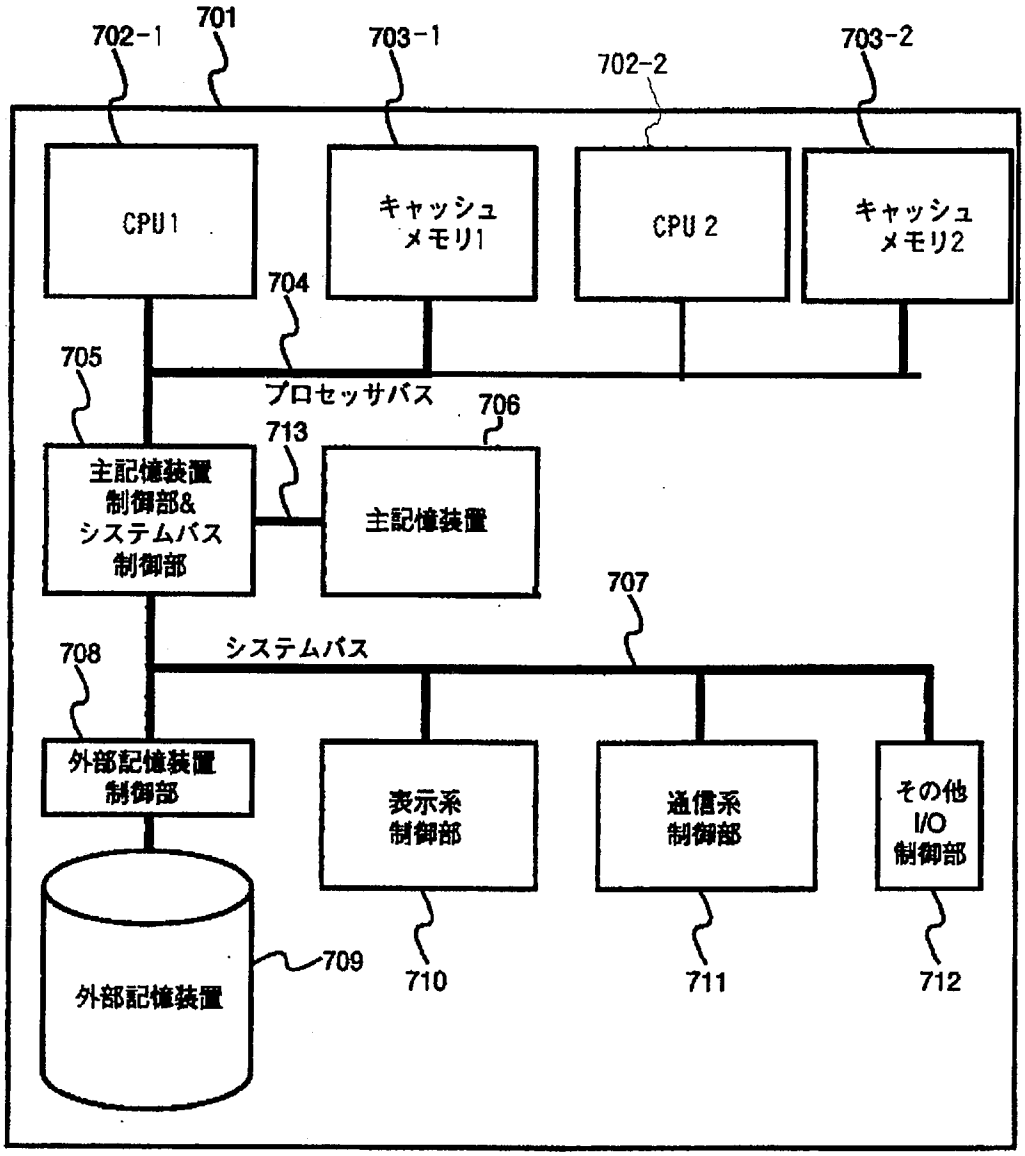
第１０図


901
902
903
907
904
磁気ディスク
ディスクシステム
コントローラ
ホストシステム
暗号化ファイル
暗号化
ファイル配置情報
空領域
検索
暗号化ファイル
ファイル識別子
暗号化
復号化
ファイル配置情報
1001
905
908

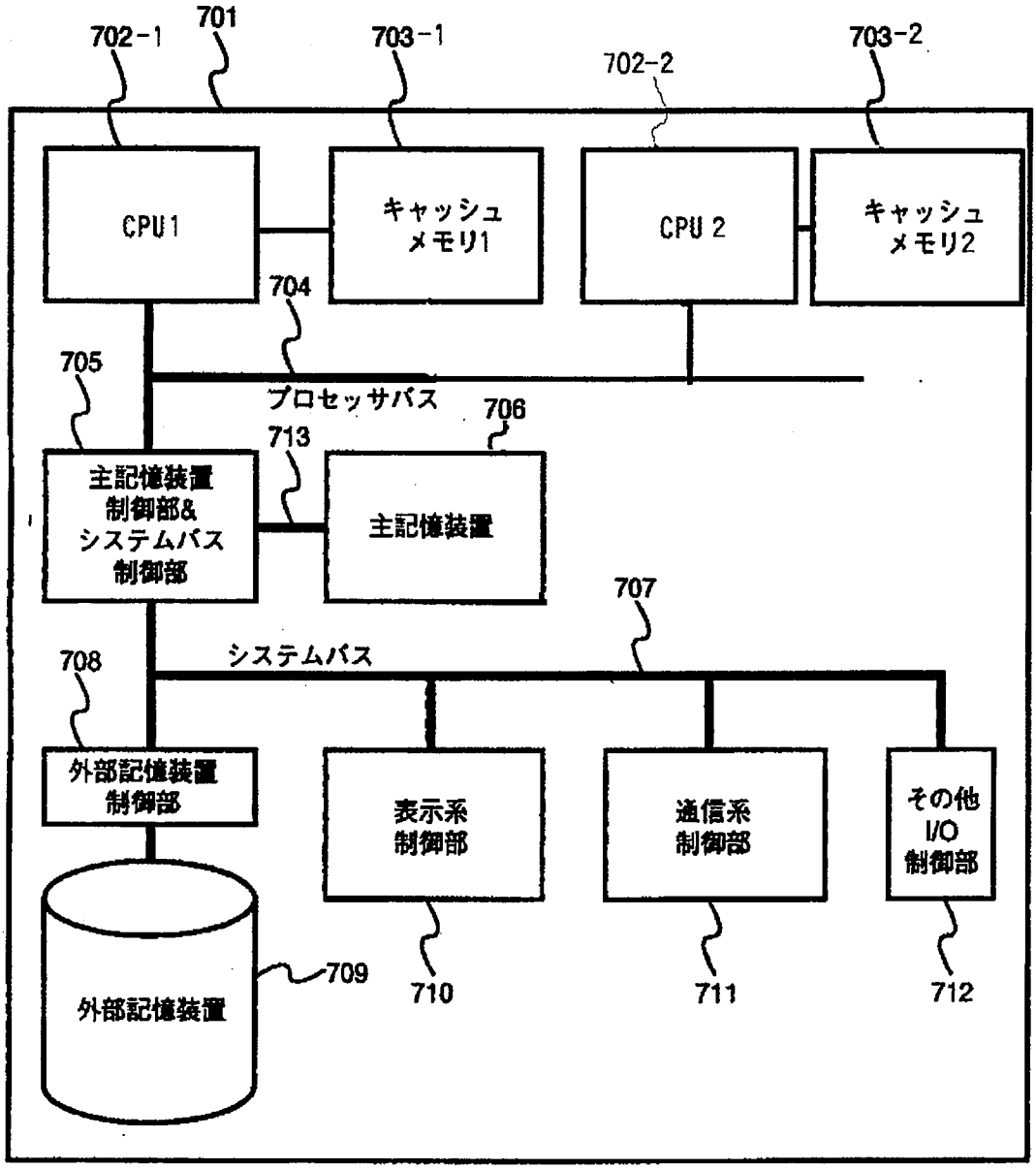
第１１図


1101
ディスクシステムコントローラ
1114
1115
1112
1116
磁気ディスク
インタフェース
ホストシステム
インタフェース
ホストシステム
1117
暗号化
ファイル
配置情報
磁気ディスク
1113
外部バス制御部
1105
1109
マイクロ
プロセッサ
1107
暗号処理
ハードウェア
暗号処理
アルゴリズム
ROM
1106
1110
1111
暗号化
ファイル
配置情報
1118
鍵
保管
領域
ファイル
配置情報
1119
1102
1108
メモリ
CPU
1104
1103

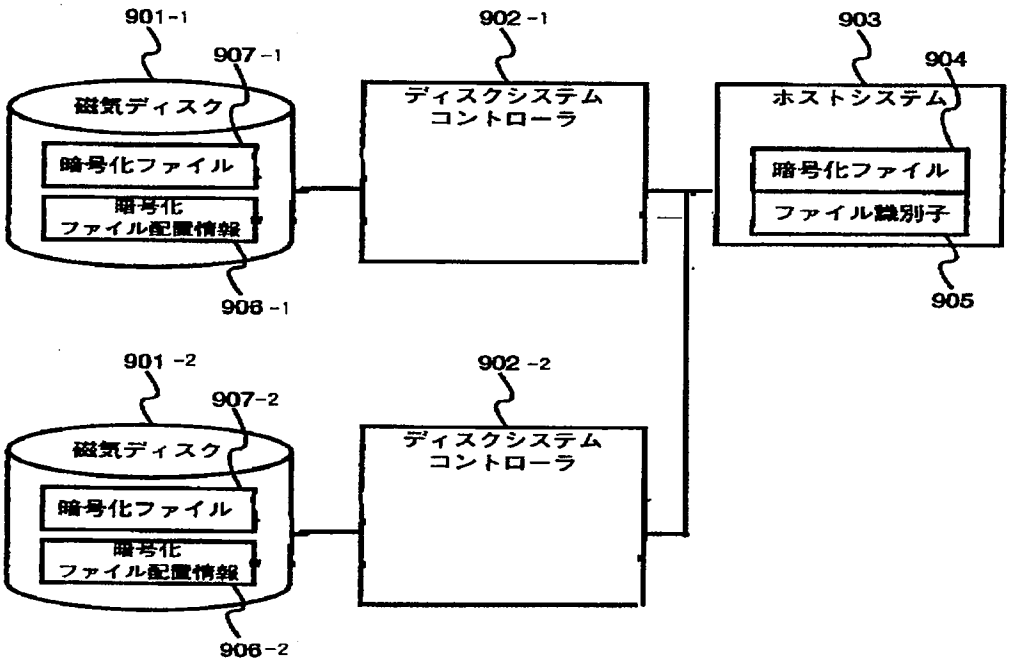
第１２図


702-1
701
703-1
702-2
703-2
CPU1
キャッシュ
メモリ1
CPU 2
キャッシュ
メモリ2
704
705
プロセッサバス
706
713
主記憶装置
制御部&
システムバス
制御部
主記憶装置
707
708
システムバス
外部記憶装置
制御部
表示系
制御部
通信系
制御部
その他
I/O
制御部
709
外部記憶装置
710
711
712

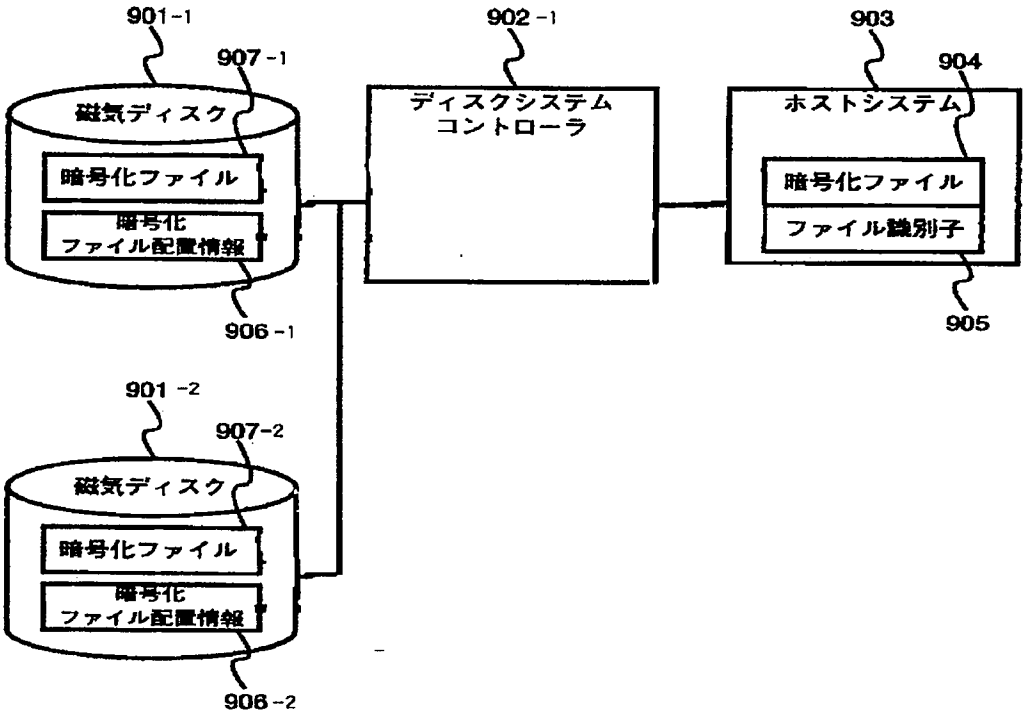
第１３図


701
702-1
703-1
702-2
703-2
CPU1
キャッシュ
メモリ1
CPU 2
キャッシュ
メモリ2
704
705
プロセッサバス
706
713
主記憶装置
制御部&
システムバス
制御部
主記憶装置
707
708
システムバス
外部記憶装置
制御部
表示系
制御部
通信系
制御部
その他
I/O
制御部
709
外部記憶装置
710
711
712

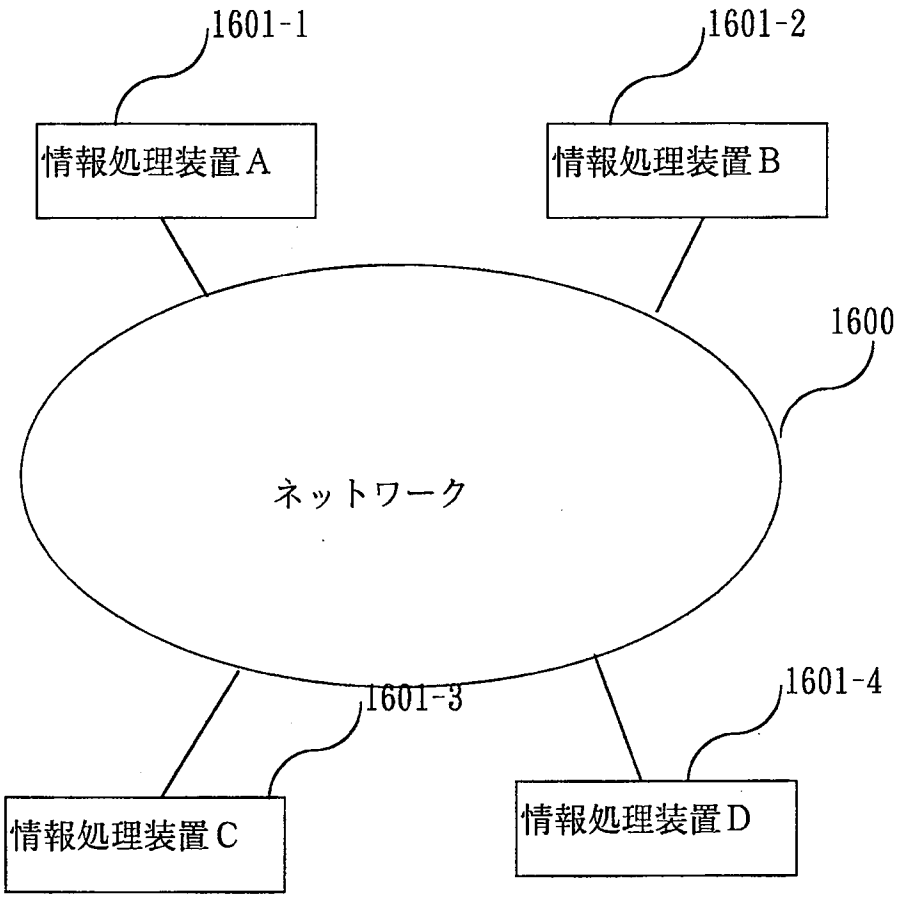
第１４図


901-1
907-1
磁気ディスク
暗号化ファイル
暗号化
ファイル配置情報
906-1
902-1
ディスクシステム
コントローラ
903
904
ホストシステム
暗号化ファイル
ファイル識別子
905
901-2
907-2
磁気ディスク
暗号化ファイル
暗号化
ファイル配置情報
906-2
902-2
ディスクシステム
コントローラ

第１５図


901-1
907-1
磁気ディスク
暗号化ファイル
暗号化
ファイル配置情報
906-1
902-1
ディスクシステム
コントローラ
903
904
ホストシステム
暗号化ファイル
ファイル識別子
905
901-2
907-2
磁気ディスク
暗号化ファイル
暗号化
ファイル配置情報
906-2

第１６図


1601-1
1601-2
情報処理装置Ａ
情報処理装置Ｂ
1600
ネットワーク
1601-3
1601-4
情報処理装置Ｃ
情報処理装置Ｄ

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP99/01402

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[6] G06F15/00, G06F12/14, H04L9/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[6] G06F15/00, G06F12/14, H04L9/10

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1926-1996 Toroku Jitsuyo Shinan Koho 1994-1999
Kokai Jitsuyo Shinan Koho 1971-1999 Jitsuyo Shinan Toroku Koho 1996-1999

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP, 64-4194, A (Hitachi,Ltd., Hitachi Tohbu Semiconductor,Ltd.), 14 February, 1989 (14. 02. 89) (Family: none)	1-12
Y	JP, 2-297626, A (NEC Corp.), 10 December, 1990 (10. 12. 90) (Family: none)	1-9
Y	JP, 4-149652, A (Mitsubishi Electric Corp.), 22 May, 1992 (22. 05. 92) (Family: none)	1-9
Y	JP, 5-314014, A (Toshiba Corp.), 26 November, 1993 (26. 11. 93) (Family: none)	10-12
Y	JP, 9-44407, A (NEC Engineering K.K.), 14 February, 1997 (14. 02. 97) (Family: none)	10-12

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 June, 1999 (11. 06. 99)	22 June, 1999 (22. 06. 99)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

国際調査報告

国際出願番号　PCT／JP99／01402

A.　発明の属する分野の分類（国際特許分類（IPC））

Int. Cl[6]　G06F 15/00, G06F 12/14, H04L 9/10

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl[6]　G06F 15/00, G06F 12/14, H04L 9/10

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1926－1996年
日本国公開実用新案公報	1971－1999年
日本国実用新案登録公報	1996－1999年
日本国登録実用新案公報	1994－1999年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	JP，64－4194，A（株式会社日立製作所，日立東部セミコンダクタ株式会社） 14.　2月.1989（14.02.89）（ファミリーなし）	1-12
Y	JP，2－297626，A（日本電気株式会社） 10.12月.1990（10.12.90）（ファミリーなし）	1-9
Y	JP，4－149652，A（三菱電機株式会社） 22.　5月.1992（22.05.92）（ファミリーなし）	1-9
Y	JP，5－314014，A（株式会社東芝） 26.11月.1993（26.11.93）（ファミリーなし）	10-12

☒ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日 11.06.99	国際調査報告の発送日 22.06.99
国際調査機関の名称及びあて先 日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員） 中里 裕正　5M　9364 電話番号　03－3581－1101　内線　3599

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ９９／０１４０２

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ｙ	ＪＰ，９－４４４０７，Ａ（日本電気エンジニアリング株式会社） １４．　２月．１９９７（１４．０２．９７）（ファミリーなし）	10-12